87

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/905,341	07/14/2001	Trevor Yann	655/62437	3754

7590 07/15/2005

Richard F. Jaworski
Cooper & Dunham LLP
1185 Avenue of the Americas
New York, NY 10036

EXAMINER	
NGUYEN, MINH DIEU T	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 07/15/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/905,341	**Applicant(s)** YANN ET AL.	
	Examiner Minh Dieu Nguyen	**Art Unit** 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 April 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the communication dated April 14; 2005.

Claims 1-19 are pending.

Response to Arguments

2. Applicant's arguments filed April 14, 2005 have been fully considered but they are not persuasive.

Applicant argues that Nachenberg fails to teach the claimed limitation 1, Nachenberg teaches detecting polymorphic viruses without emulating unnecessarily large numbers of instructions (i.e. eliminating of certain polymorphic viruses from consideration prior to emulation, see Remarks, pages 7-8).

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., detecting polymorphic viruses without emulating unnecessarily large numbers of instructions are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Nachenberg clearly teaches emulating a first predetermined number of instructions of the computer program (col. 6, lines 45-48; col. 3, lines 37-53).

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 1-19 are rejected under 35 U.S.C. 102(b) as being anticipated by Nachenberg et al. (5,826,013).

As to claim 1, Nachenberg teaches a method of detecting polymorphic viral code in a computer program, comprising the steps of:

(a) emulating a first predetermined number of instructions of the computer program (col. 6, lines 45-48);

(b) collecting information corresponding to a state of a plurality of registers and/or flags after each emulated instruction execution (col. 9, lines 24-32; col. 12, line 64 thru col. 13, line 10); and

(c) determining a probability that the computer program contains polymorphic viral code based on an heuristic analysis of the collected register/flag state information (col. 3, lines 37-53; col. 9, lines 24-32; col. 12, line 64 thru col. 13, line 10).

As to claim 2, Nachenberg teaches emulating a second predetermined number of instructions if the probability determined in step (c) is above a predetermined threshold, wherein the second predetermined number of instructions is greater than the first predetermined number of instructions (col. 3, lines 37-53).

As to claim 3, Nachenberg teaches the second predetermined number of instructions corresponds to execution of a polymorphic decryptor (col. 8, lines 51-65).

As to claim 4, Nachenberg teaches monitoring the plurality of registers and/or flags for improper register/flag usage (col. 3, lines 37-53; col. 9, lines 24-32; col. 12, line 64 thru col. 13, line 10).

As to claim 5, Nachenberg teaches maintaining, for each of the plurality of registers and/or flags, a corresponding count of a number of times that the register/flag was improperly used during the emulation of instructions in steps (a) (col. 3, lines 44-53).

As to claim 6, Nachenberg teaches monitoring operand values of the instructions emulated in step (a) (col. 3, lines 37-53; col. 9, lines 24-32; col. 12, line 64 thru col. 13, line 10).

As to claim 7, Nachenberg teaches detecting when operand values of an instruction which is set is not used by the instruction (col. 9, lines 24-32; col. 11, lines 23-28).

As to claim 8, Nachenberg teaches detecting when an undefined operand of an instruction is used by the instruction (col. 3, lines 1-36).

Claim 9 is a program storage device claim that is substantially equivalent to method claim 1, therefore claim 9 is rejected for the same reasons.

Claim 10 is a computer system claim that is substantially equivalent to program storage claim 9, therefore claim 10 is rejected for the same reasons.

Claim 11 is a computer data signal claim that is substantially equivalent to program storage claim 9, therefore claim 11 is rejected for the same reasons.

Claim 12 is an apparatus claim that is substantially equivalent to program storage claim 9, therefore claim 12 is rejected for the same reasons.

Apparatus claims 13-19 are substantially equivalent to method claims 2-8 respectively, therefore claims 13-19 are rejected for the same reasons.

Conclusion

5. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dieu Nguyen whose telephone number is 571-272-3873. The examiner can normally be reached on M-F 6:00-2:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

6. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

Minh Dieu Nguyen
Examiner
Art Unit 2137

mdn
7/11/05

Matthew D. Smithers
MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137